STATEMENT

OF

CATHERINE A. ALLEN
CHIEF EXECUTIVE OFFICER

BITS
THE TECHNOLOGY GROUP
FOR
THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE
JOINT ECONOMIC COMMITTEE
UNITED STATES CONGRESS

June 21, 2001

TESTIMONY OF CATHERINE A. ALLEN, CEO, BITS

Good morning, Mr. Chairman, and other members of the Joint Economic Committee. I am Peggy Lipps, Senior Director of Security and Risk Assessment Initiatives for BITS, the Technology Group for The Financial Services Roundtable. I am here to present testimony on behalf of Catherine Allen, CEO of BITS, who regrets not being able to be here in person. BITS was established in late 1996 to focus on critical issues at the interface of technology, commerce and financial services. BITS is a not-for-profit industry consortium and a sister organization to The Financial Services Roundtable. BITS and the Roundtable's membership is currently open to the largest integrated financial services companies in the US. These include such diverse organizations as Citigroup, Bank of America, J.P. Morgan Chase & Co., Wells Fargo & Co., Capital One, Chubb, Prudential, State Farm, Raymond James and Goldman Sachs. BITS is not a lobbying organization; instead, we serve as a business and technology strategy consortium.

The BITS Board of Directors is chaired by James H. Blanchard, Chairman and CEO of Synovus Financial Corp. The BITS Board is composed of the Chairmen or CEOs of 20 of the largest integrated financial services companies in the US, representing the banking, insurance and securities industries. Representatives of the American Bankers Association and the Independent Community Bankers of America also sit on the Board, assuring representation of financial institutions of all sizes. The heads of information security for 50 of our member institutions serve as the members of the BITS Security and Risk Assessment Steering Committee.

Thank you for the invitation to appear before the Joint Economic Committee today. We would also like to acknowledge Senator Bennett personally. The Senator has met with BITS on the topic of security and risk management and was a keynote speaker, along with former Senator Sam Nunn, at the launch of the BITS Financial Services Security Lab.

I would like to discuss with you today these three major topics:

- **The seriousness with which our industry takes the issue of critical infrastructure protection** because of the growing interdependencies between core sectors such as telecommunications, transportation, electric power and financial services. E-commerce demands a partnership between providers, customers, and all the intermediaries to ensure a secure environment.
- **The leadership role that BITS and the financial services industry is taking** in areas of security and risk management and how we are sharing that expertise with other sectors through the Partnership for Critical Infrastructure Security (PCIS).
- **What we believe Congress can and should do** to address the issue of critical infrastructure security, including:
    - Supporting public/private sector partnerships;
    - Aligning laws and regulations;
    - Promoting regulatory equality; and
    - Encouraging education and understanding.

FINANCIAL SERVICES SECTOR LEADERSHIP IN RISK MANAGEMENT

The financial services sector has long been a leader in security assurance. Vigilance and the dedication of enormous resources over time have allowed us to develop a wealth of expertise, experience and talent to address issues of security, risk management and protection against crimes such as fraud.

Online delivery of financial services depends on large and complex public as well as private networks—security must be built into every part of the system. The shift to electronic, and increasingly mobile, commerce extends the need for security all the way to the individual customer and to the implementing networks, servers, software and devices. Our industry is focused on protection of the integrity of the infrastructure for physical, as well as electronic, delivery of financial services and has taken steps to assure that the global architecture for financial transactions is as safe, secure and sound as possible. Our efforts and actions serve the entire e-commerce environment.

PUBLIC/PRIVATE SECTOR PARTNERSHIP

The financial services industry is dependent on the other core infrastructures—electric power, telecommunications, transportation—and they depend on financial services for their core operations. This interdependency is a key concern of both the private sector and the federal government, and the main reason Presidential Decision Directive 63 recommended a public-private partnership to address the issue.

The key to ensuring security for all participants in e-commerce is strong cross-sector involvement. No one sector can address these issues alone. Neither can the government. Models can be developed, and are being developed within the financial services sector, to assist all sectors in working cooperatively to ensure the safety, soundness and security of the infrastructures that collectively support our national economy. Appropriate cross-sector actions include interdependency vulnerability analysis, information sharing, awareness building, identification of research and development gaps, and contributions to the development of an informed and integrated national plan that both industry and government can use as a business case for action.

BITS' CROSS-SECTOR APPROACH

Inclusion: We involve all stakeholders in the process. This means including government agencies, regulators, and vendors in our security-related initiatives and Working Groups. We work closely with other industry groups on security-related issues. We have a strong relationship with financial institutions of all sizes, in part as a result the active participation of the Independent Community Bankers of America, American Bankers Association, America's Community Bankers and CUNA in BITS' Working Groups.

Education: We make sure that stakeholders are working from the same basis of knowledge. We serve in an educational role for our members, representatives of regulatory agencies, Members of Congress, industry participants, and consumers about risk issues and how to make the e-commerce and mobile commerce environments more safe and secure.

Proactive Efforts: We address the vulnerabilities involved with the financial services sector's infrastructure—including technology, processes, people and insurance—through appropriate industry-driven efforts such as establishing self-regulatory guidelines and testing products against security criteria.

Some examples of efforts to create and build a strong public/private sector partnership include:

- **PCIS**: Founded in 1999, the purpose of the Partnership for Critical Infrastructure Security (PCIS) is to promote and assure reliable provision of critical infrastructure services through cross-sector coordination. The PCIS is embarking on a series of interdependency vulnerability exercises, broadening early efforts by the Department of Energy, where it will investigate critical dependencies and nodes, meet points of contact from the stakeholder organizations, and develop remediation and protection plans. BITS is a founding member.
- **CIAO**: The Critical Infrastructure Assurance Office (CIAO) was created in response to Presidential Decision Directive 63 in May of 1998 as a mechanism to assist in the coordination of the federal government's initiatives on critical infrastructure protection. BITS has been involved since its inception.
- **FS/ISAC**: The Financial Services/Information Sharing and Analysis Center (FS/ISAC) is a facility for anonymously gathering information on threats, vulnerabilities, incidents, resolutions, and solutions. BITS has been involved since its inception and has encouraged industry participation.
- **BITS' Financial Services Security Laboratory**: Established by BITS in 1999, the Lab tests e-commerce products against the financial services community's strong security requirements.
- **BITS' Self-Regulatory Guidelines** vetted with regulators and industry stakeholders
- **Strategic Partnerships** with the US Navy and DOD
- **BITS' Briefings** to regulators and Members of Congress
- **BITS' White Papers and Alerts** to the financial services industry

BITS' APPROACH TO THE ISSUE OF CRITICAL INFRASTRUCTURE PROTECTION

BITS uses a risk management model focused on technology, processes and people to drive our security and infrastructure protection initiatives.

Technology—Our goal is to ensure that technology products developed for our industry incorporate features and functionality that comply with meaningful security criteria required for financial services. Vendors do not always include security protections because of the associated costs, time to develop new versions of products or lack of understanding of the risks to financial institutions. BITS takes a market-driven approach to influencing vendors and the product development process. Some examples of those efforts include the following.

- **BITS Financial Services Security Lab** and **BITS Tested Mark**: The BITS Security Lab tests e-commerce products against security criteria developed by the

financial services industry. Through workshops, the 12 product profiles against which products are tested are vetted with government agencies, including Navy and Defense, as well as vendors. The first product to pass the testing process and receive the BITS Tested Mark is the Hewlett-Packard Company's HP Virtualvault 4.0.

- **BITS Wireless Technologies RFI:** Through an RFI (Request for Information) process, BITS has engaged over 70 wireless carriers, solutions providers and device manufacturers in a process to identify and address security and end-to-end reliability issues related to delivery of financial services in mobile commerce.

Processes— As important as the technologies we use, the processes we implement create the critical infrastructure in which we operate. Processes are more difficult to test but, using self-regulatory guidelines and best practices, we can dramatically enhance the security of the infrastructure. Examples of how the industry has addressed security processes include the following.

- **BITS Voluntary Guidelines for Aggregation Services**: A good model for how the financial services industry has created self-regulatory guidelines built upon a public/private sector partnership is the work BITS just completed on aggregation services. Online financial aggregation services allow consumers to see a consolidated view of all their account information. Increasingly the services will enable financial transactions as well as provide personalized financial planning services. Over 215 executives from 80 organizations—including regulators, government agencies, technology providers and financial institutions—created business guidelines for delivering aggregation services. The *BITS Voluntary Guidelines for Aggregation Services* address security, privacy, customer education and disclosures, data feed standards, and related legal and regulatory issues.
- **BITS Framework for Managing Information Technology (IT) Service Provider Relationships**: The financial services industry increasingly relies on information technology (IT) service providers to support the online delivery of its products and services. This marks a directional change. There is a heightened awareness of the need for financial institutions to assess and manage the risks associated with use of such service providers. In the next few months, BITS will publish guidelines for selecting and managing IT service providers based on industry best practices, the security and privacy requirements of the Gramm-Leach-Bliley Act and the FFIEC guidelines. BITS' Guidelines provide a framework for service providers and financial institutions to establish appropriate controls. These Guidelines initially have been vetted with a few regulators and were vetted by a broader audience of financial institutions, vendors and regulators in June.
- **Authentication/E-SIGN Working Group**: Through a process that maps key financial transactions, a diverse cross-industry effort is under way to address the need for authentication processes, including the levels of risk and appropriate solutions—technological or other—to offset potential security breaches. Ultimately, we hope to drive the development and implementation of open, interoperable standards for authentication.

People—People we employ, vendors we use, customers we serve and the agencies that regulate us have an impact on the level of security of the financial services industry's infrastructure. Through research and educational programs, often conducted in concert with

organizations such as BAI, ECCHO, the American Bankers Association, the Independent Community Bankers of America and other industry groups, we are ensuring that the knowledge and skills, necessary to work as informed partners with the financial services industry, are provided to address security and risk management issues. We have participated in educational programs sponsored by, or developed for, federal agencies such as the OTS, OCC, Federal Reserve Board and the US Patent and Trademark Office. We speak at more than 100 industry events each year.

Insurance—Even with the best of processes and products, no system will be 100% secure. There will be gaps. Increased concerns over security vulnerabilities—and the complexity of identifying and quantifying vulnerabilities from e-commerce related activities—are driving a need to review the role of insurance. This is both as a solution within an organization's overall risk management strategy and as an incentive to raise the level and quality of security within the interdependent critical infrastructure networks. BITS has organized an initiative to help define and fill the gaps and we have been working with the Critical Infrastructure Assurance Office (CIAO) to address the role of public and private sector involvement.

CHALLENGES

As we work within our industry sector, and with other sectors, we have encountered some obstacles to cross-sector cooperation that we would like to bring to your attention. We believe we can overcome most of these, but some may require assistance from Members of Congress.

- **Awareness of the growing impact of our nation's dependency on automation and interlinked networks, and our interdependency among sectors, is not universal.** The PCIS, working with the Critical Infrastructure Assurance Office (CIAO) has developed a broad awareness and outreach plan that will target several key groups, from CEOs and government executives to their staffs, auditors and systems administrators. Because our economy is reliant on this automation, interlinked networks and interdependent infrastructures for productivity improvements, it is important not to view critical infrastructure protection through only a national security or law enforcement lens. Critical Infrastructure Protection is necessary to assure all the national benefits of a robust economy. Thus, it is essential that national preparedness leadership responsibility be recognized and that there be close coordination of the appropriate government communities with that leadership.
- **There are significant real and perceived barriers to information sharing and vulnerability assessments.** The Freedom of Information Act (FOIA) was designed to provide information to the public on government actions, but some companies are reluctant to share vulnerability information with the government for fear of a competitor's subsequent FOIA request. Also, some public utilities are reluctant to conduct vulnerability assessments because their state laws require full disclosure to the public—and such disclosure may undermine consumer confidence, which would vastly complicate the efforts to make improvements. Sunshine laws vary widely among the states, complicating the issue even further.
- **The Internet knows no borders, but the various national defense and law enforcement organizations around the world are bound by archaic physical limitations.** Physical jurisdiction is irrelevant in coping with crimes conducted across borders in minutes and seconds. Several efforts are underway to address the

international dimension of critical infrastructure protection, and the Congress should be made aware of their implications.

- **The network security "skills gap" is still increasing.** The National Security Agency's "Centers of Excellence in Information Assurance" has identified 23 universities with outstanding programs, and the nascent "Cybercorps" scholarship-for-service program is a good start, but more must be done.
- **Market forces alone will not provide sufficient research and development to meet sector economic security or national security needs**. The PCIS is conducting a gap analysis of existing and planned critical infrastructure protection research by industry, academia and government. Purposes of this study are to identify areas of duplication of effort and highlight needs identified by sectors and government that will not be met by the market. The government could use that report to provide incentives or directly fund needed research to close that gap. Further, attacks on our critical infrastructure may require cohesive and comprehensive rapid response plans, similar in scope to those used by emergency management agencies when addressing natural disasters.
- While financial institutions are increasingly providing educational support to their customers—for example, with recommendations for protecting their personal computers' security when conducting online financial transactions—**much more cross-sector and pervasive education is needed for the general public**.

RECOMMENDATIONS

We propose that you and other Members of Congress consider the following recommendations in approaching this critical issue of infrastructure protection:

- **Support Public/Private Sector Partnerships**: The kinds of voluntary guidelines and business practices we have described, as well as the work of the PCIS, have in fact already enabled effective self-regulation and cooperation across sectors. We believe that this strong public/private partnership will continue to work and should be supported through national leadership and government community organizations.
- **Align Laws and Regulations**: We have taken the responsibility to make coherent industry-based recommendations available throughout the financial services sector. We believe the government can play a similarly effective role in rationalizing the national legal and regulatory framework across sectors. A great deal can be lost, in effectiveness and in dollars, when institutions have to respond to a wide variety of conflicting laws and regulations on security and privacy. For example, there may be a need for federal pre-emption of state laws in critically important areas such as privacy and security. The bottom line is that differing, and sometimes conflicting, laws and regulations dissipate our resources and actually increase security risks and vulnerabilities.
- **Promote Regulatory Equality**: Ensure that all entities offering financial services are required to adhere to the same meaningful standards for security and privacy as do currently regulated financial institutions—especially as the line between financial institutions and IT service providers blurs.
- **Encourage Education and Understanding**: We want to continue to work collaboratively with you to foster the growth of electronic commerce in the kinds of safe, sound and secure ways that are necessary for the confidence of consumers and

the growth of our economy. We would be happy to provide briefings, prepare white papers, provide experts, and work in whatever ways are appropriate to assist you and others in understanding the critical nature and complexity of issues involved in the security of our critical infrastructures.

CLOSING THOUGHTS

Mr. Chairman and Members of the Committee, I have given you our perspective about how serious the issue of critical infrastructure protection is to the financial services industry; the leadership that BITS, the PCIS and other members of the financial and security communities have taken; and some recommendations about ways Congress might approach this issue. We believe that the strong public/private sector partnership that is emerging is the right approach. We will work with your Committee and other Members of Congress to suggest more specifically where laws and regulations need to be aligned, where regulations should be applicable in order to have all players adhere to security and risk management principles, and where further education and understanding are needed.

I want to acknowledge the cooperation and assistance of the PCIS in preparing this testimony.

Thank you for this opportunity to testify. I am happy to answer any questions you may have and we would be pleased to meet with the Committee staff or any Members personally to discuss aspects of the testimony in greater detail.

FOR ADDITIONAL INFORMATION

Catherine A. Allen, CEO
Peggy Lipps, Senior Director
BITS
The Financial Services Roundtable
805 15th Street NW, Suite 600
Washington DC 20005
(202) 289-4322 Phone
(202) 289-0193 Fax
cathy@fsround.org
peggy@fsround.org
www.bitsinfo.org

APPENDIX

THE CURRENT ENVIRONMENT IN CYBERSECURITY

While new technologies create new opportunities, they also open the door to new kinds of attacks, new threats, and new vulnerabilities. Approximately 100 types of new vulnerabilities are added monthly to Mitre's Common Vulnerabilities and Exposures (CVE) list. Attacks include cyber-extortion of stolen data, mass theft of credit card information, automated denial of service, and cases of organized hacker groups acting collaboratively to target US e-finance and e-commerce sites. All these risks have the potential to negatively affect the economy, our nation's security, and certainly consumer confidence.

The Computer Security Institute (CSI) reported in March 2001 the results of its sixth annual "Computer Crime and Security Survey." The survey confirms that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting. The most serious financial losses occurred through theft of proprietary information and financial fraud. Losses from viruses, insider abuse of network access, and system penetration by outsiders were also substantial. According to the Survey:

- "For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%)."
- 94% detected computer viruses, up from 85% in 2000.
- 40% detected system penetration from the outside, up from 25% in 2000.
- Specific to e-commerce over the Internet, 78% reported denial of service, up from 60% in 2000 and 13% reported theft of transaction information, up from 8% in 2000.

As a result of such attacks, the security products and services marketplace is predicted to grow at a rate of 28% every year through 2005. Spending on security among the largest 2500 global US-based firms will increase by 55% in the next two years.